



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,764	02/09/2004	Elias Levy	SYMAP042	8717
21912 7590 12/23/2008 VAN PELT, YI & JAMES LLP 10050 N. FOOTHILL BLVD #200 CUPERTINO, CA 95014				
EXAMINER				
BROWN, CHRISTOPHER J				
ART UNIT		PAPER NUMBER		
2434				
MAIL DATE		DELIVERY MODE		
12/23/2008		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/775,764

Applicant(s)

LEVY, ELIAS

Examiner

CHRISTOPHER J. BROWN

Art Unit

2434

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 November 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 7, 8, 13-15 and 17-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 7, 8, 13-15 and 17-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/808)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

The Request for Continued Examination has been accepted and entered.

Response to Arguments

Applicant's arguments, filed 11/20/2008 with respect to the rejection(s) of claim(s) 1 under Blake US 2004/0128543 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Becker US 2004/0139128.

Claim Rejections - 35 USC § 101

The claimed invention is directed to non-statutory subject matter. The method claim, Claim 1 must be tied to a machine or a computer readable medium for it to be statutory.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claim*** rejected under 35 U.S.C. 103(a) as being unpatentable over ***.

Claims 1-4, 7, 9, 10, 15, 18-20, 23, 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Becker US 2004/0139128.

As per claim 1, 23, Blake teaches deploying a honey pot (Fig 4, system for morphing a honeypot on a dynamic and configurable basis, administrator configures honeypot [0011], [0036]. Blake teaches detecting a breach of the honey pot (suspicious requests, acts to compromise honeypot, client system probing for vulnerability, attacks) [0038], [0070], [0075], [0084]. Blake teaches capturing the state of the honeypot including creating a copy of the data associated with a compromised honeypot (activity logs) [0040]. Blake teaches automatically redeploying the honey pot [0037], [0076].

Becker teaches reinitializing to an initial state via an image [0151], [0163].

It would have been obvious to one of ordinary skill in the art to use the image of Becker with the redeployment of Blake because it would restore the honeypot after a compromise.

As per claim 2 Blake teaches analyzing the breach (analysis operations, analyzing requests) [0037], [0075].

As per claim 3 Blake teaches automatically analyzing the breach (automatic analysis), Figure 4, [0037], [0075].

As per claim 4 Blake teaches the breach is automatically detected (determination is made as to whether a probe has been detected) [0070], [0075].

As per claim 7, Blake teaches configuring the honey pot (configuration phase (step 402)) [0037].

As per claim 9 Blake teaches the honey pot is a physical machine (implemented in hardware) [0026].

As per claim 10 The method of claim 1, wherein the honey pot is a virtual machine (virtual directories, emulated)[0038].

As per claim 15 Blake teaches the detecting is based on an elapsed time (track suspicious client requests over time) [0070].

As per claim 18 Blake teaches saving state information associated with the honey pot (activity logs) [0040].

As per claim 19 Blake teaches saving state information associated with the honey pot and wherein saving and redeploying occur in parallel (all activity, actions taken by emulated services, or honeypot as whole, is logged) [0040].

As per claim 20, Blake teaches analyzing the breach and redeploying occur in parallel (analysis and reconfiguration operations performed at the same time) [0037].

As per claim 24, Blake teaches deploying a honey pot (Fig 4, system for morphing a honeypot on a dynamic and configurable basis, administrator configures honeypot

[0011], [0036]. Blake teaches detecting a breach of the honey pot (suspicious requests, acts to compromise honeypot, client system probing for vulnerability) [0038], [0070], [0075]. Blake teaches automatically redeploying the honey pot (automatic reconfiguration operations, reconfigured to present information reflecting a different vulnerability) [0037], [0076]. Blake teaches the honeypot is implemented using a processor and memory coupled to the processor (CPU, disk units) [0026].

Claims 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Becker US 2004/0139128 in view of Fagone US 2004/0078592.

As per claim 6 Blake does not teach shutting down the honey pot.

Fagone teaches shutting down the honeypot (disconnecting from network) [0017].

It would have been obvious to one of ordinary skill in the art to use the shut down method of Fagone in case a honeypot becomes a danger to the network [0017].

Claim 8, is rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Becker US 2004/0139128 in view of Schlereth “Analysis of a Compromised Honeypot on a Cable Modem”.

As per claim 8 Blake does not teach copying a honey pot image.

Infocus teaches creating and copying a honeypot image (creating an image of a compromised system for investigation, Pages 21-24).

It would have been obvious to one of ordinary skill in the art to use a honeypot image because it limits the chance of destroying evidence on the compromised system (page 24).

Claims 13, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Becker US 2004/0139128 in view of Lewis US 2003/0110396.

As per claim 13 Blake fails to teach detecting is based on the number of outgoing connections detected. Lewis teaches detecting is based on the number of outgoing connections detected (large number of IP requests) [0079].

It would have been obvious to one of ordinary skill in the art to use the detection of Lewis in the system of Blake to detect Denial of Service attack attempts.

As per claim 14 Blake fails to teach detecting is based on the number of incoming connections detected. Lewis teaches detecting a breach based on the incoming connections detected (abnormally large connection attempts to target) [0062].

It would have been obvious to one of ordinary skill in the art to use the detection of Lewis in the system of Blake to detect Denial of Service attack attempts.

Claim 17, is rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Becker US 2004/0139128 in view of INFOCUS:The HoneyNet Project

As per claims 17 Blake does not specify an operating system.

Infocus teaches the honey pot runs a Linux operating system(linux, page 3). It would have been obvious to one in the art to use the multiple OS of Infocus with the honeypot of Blake because it provides support to create a honeypot for a wide range of users.

Claims 21, and 22, are rejected under 35 U.S.C. 103(a) as being unpatentable over Blake US 2004/0128543 in view of Becker US 2004/0139128 in view of Turk US 2005/0108415

As per claims 21, and 22, Blake does not teach mapping an IP address to a honeypot.

Turk teaches receiving an incoming connection associated with an IP address(ping a given IP address)[0071]. Turk teaches mapping the IP address to the honey pot (honeypot responds to unrouted IP address requests) [0071]. Turk teaches releasing the IP address mapping and mapping another IP address to the honey pot (honeypot accepts any IP address request that is not stored in the routing table, thus it will remap to a different IP if a different unrouted destination IP request arrives) [0071].

It would have been obvious to one of ordinary skill in the art to use the IP mapping of

Turk with the system of Blake because it tricks a malicious user into thinking they have successfully compromised their target destination IP.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/775,764
Art Unit: 2434

Page 9